SignNow

Data Processing Addendum

This Data Processing Addendum ("**DPA**") amends and forms part of the Agreement (as defined below) between Provider and you as a user of Provider's Services ("**Customer**").

1. Definitions

For purposes of this DPA, the following terms will have the following meaning:

- "**Agreement**" means any agreement between Provider and Customer for the Services, regardless of a title, such as "Order Form," "Sales Order," "Terms of Use," "Terms of Service," "SaaS Agreement," or "Services Agreement".
- "**Controller**" has the meaning defined in GDPR.
- "**Customer Account and Usage Data**" means information about Customer that Customer provides to Provider in connection with the creation and administration of an account, such as the first and last names, username, email address, and billing and payment information of individuals associated with an account. This also includes statistical or analytic information related to the Customer's use of the Service and any derived data.
- "**Customer Data**" means the data Processed by Provider in connection with the provision of the Services, as described in the Agreement, excluding Customer Account and Usage Data.
- "**Customer Personal Data**" means Customer Data, which consists of Personal Data.
- "**Data Protection Law(s)**" means any applicable legislation or regulation relating to the processing of personal data, including (a) the California Consumer Privacy Act and its implementing regulations; (b) the GDPR (as defined below) and related data protection and privacy laws of the member states of the European Economic Area; (c) the Data Protection Act 2018 of the United Kingdom ("UK GDPR"); and (d) the Swiss Federal Act on Data Protection ("Swiss DPA"), each as applicable and as amended, repealed, consolidated, or replaced from time to time.
- "**European Area**" means the European Union, European Economic Area, Switzerland, and the United Kingdom of Great Britain and Northern Ireland ("UK").
- "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- "**Personal Data**" means any information relating to an identified or identifiable natural person that Provider processes on behalf of Customer under the Agreement.
- "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the confidentiality, availability, or integrity of Customer Data or confidential information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other similar incidents.
- "**Process**" or "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- "**Restricted Transfer**" means (a) where the GDPR applies, a transfer of Customer Personal Data or Customer Account and Usage Data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (b) where the Swiss DPA applies, a transfer of Customer Personal Data or Customer Account and Usage Data from Switzerland to a country that is not subject to an adequacy determination by the Swiss Federal

Data Protection and Information Commissioner; and (c) where the UK GDPR applies, a transfer of Customer Personal Data or Customer Account and Usage Data from the UK to a country that is not the subject of adequacy regulations under section 17A of the United Kingdom Data Protection Act of 2018.

- "**Standard Contractual Clauses**" means (a) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 ("UK SCCs"); and (c) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs"), each as may be updated from time to time.

- "**Third Country**" means countries which, as may be required by applicable Data Protection Laws, have not received an adequacy decision from an applicable authority relating to cross-border data transfers of Personal Data, including regulators such as the European Commission, UK ICO, or Swiss FDPIC.

Capitalized terms used but not defined above will have the meanings outlined in the Agreement. Except as otherwise provided in this DPA, the terms "Business", "business purpose", "commercial purpose", "Contractor", "Controller", "Process", "Processor", "Subprocessor", "Data Subjects", "deidentify", "Sell", "Service Provider", "Share", and "Third Party" have the same meaning as in the applicable Data Protection Laws, and their cognate terms will be construed accordingly. All other capitalized terms have the same meaning as in the Agreement.

2. Roles of the Parties

2.1. Customer Personal Data. The parties agree that Provider is a Processor with respect to the Processing of Customer Personal Data.

2.2. Account and Usage Data. The Parties agree that Customer and Provider are independent Controllers with respect to the Processing of Customer Account and Usage Data, and each Party will comply with its obligations as a Controller and agrees to provide reasonable assistance to the other Party when required by Data Protection Laws. With respect to Customer Account and Usage Data, this DPA does not apply except for Section 7.

2.3. The purpose of Processing under this DPA is to provide the Services under the applicable Agreement(s). Schedule A (Description of Processing and Transfer Details) describes the subject matter and details of the Processing of Personal Data.

3. Customer Responsibilities

3.1. Customer agrees that (a) it must comply with its obligations as a Controller under the GDPR and other Data Protection Laws where such concept is recognized in respect of its processing of personal data and any processing instructions it issues to the Provider as referred to in Section 4.1; (b) it has provided notice and obtained all consents and rights required by the Data Protection Laws for the Provider to process Customer Personal Data pursuant to the Agreement and this DPA; and (c) the processing of Customer Personal Data by the Provider in compliance with the documented instructions of Customer under Section 4.1 will have a lawful basis of processing pursuant to Article 6 of the GDPR and other Data Protection Laws that require a lawful basis of processing.

3.2. If Customer is a Processor, Customer represents and warrants to the Provider that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of the Provider as another processor, have been duly authorized by the relevant Controller. Customer must indemnify, defend, and hold the Provider harmless against any claims, actions, proceedings, expenses, damages, and liabilities (including without limitation any governmental investigations, complaints, and actions) and reasonable attorneys' fees arising out of Customer's violation of this Section. Notwithstanding anything to the contrary in the Agreement, Customer's indemnification obligations under this Section will not be subject to any limitations of liability in the Agreement.

4. Data Processing and Protection

4.1. Customer instructs Provider to Process Customer Personal Data to provide the Services as documented in the Agreement, unless otherwise required by applicable law. For the avoidance of doubt, this DPA will constitute Customer's documented instructions to the Provider to process Customer's Personal Data in connection with the Provider's provision of the Service to Customer. Provider must promptly inform Customer if, in the Provider's sole opinion, an instruction violates applicable law.

4.2. Where Provider Processes Customer Personal Data in its capacity as a Processor, Provider will use, retain, disclose, or otherwise Process Personal Data only as necessary to perform on behalf of Customer and for the specific business purpose of providing the Services. Provider will not "sell" the Customer Personal Data within and in accordance with the Customer's instructions, including as described in the Agreement. Provider will not Sell or Share Personal Data, nor use, retain, disclose, or otherwise Process Personal Data outside of its business relationship with Customer or for any other purpose (including Provider's commercial purpose) except as required or permitted by law. Provider will inform Customer if Provider determines that it is no longer able to meet its obligations under Data Protection Laws. Provider or where, in Provider's reasonable opinion, any of Customer's instructions infringe any Data Protection Laws. Customer reserves the right to take reasonable and appropriate steps to (i) ensure Provider's Processing of Personal Data is consistent with Customer's obligations under Data Protection Law and (ii) discontinue and remediate unauthorized use of Personal Data. Provider certifies it understands the restrictions of this Section 4.2.

4.3. Provider has a right to use Personal Data solely (i) to the extent necessary to (a) perform its obligations under the Agreement and this DPA; (b) to operate, manage, test, maintain and enhance the Services including as part of its business operations; (c) to disclose aggregate statistics about the Services in a manner that prevents individual identification or re-identification of Customer, Customer Data, Personal Data, including without limitation any individual device or individual person; and/or (d) protect the Services from a threat to the Services or Personal Data; or (ii) if required by court order of a court or authorized governmental agency, provided that prior notice first be given to Customer; (iii) as otherwise expressly authorized by the Agreement, this DPA, or Customer.

4.4. Provider will not combine Personal Data which Provider Processes on Customer's behalf, with Personal Data which it receives from or on behalf of another person or persons, or collects from its own interaction with individual, provided that Provider may combine Personal Data to perform any business purpose permitted or required under the Agreement to perform the Services.

4.5. Provider will use commercially reasonable efforts to ensure that persons authorized by Provider to Process any Customer Personal Data are subject to appropriate confidentiality obligations.

4.6. Provider will, taking into account the nature of the processing, use commercially reasonable efforts to assist Customer, at Customer's expense, by appropriate technical and organizational measures, to the extent possible, in fulfillment of Customer's obligation to respond to requests for exercising the data subjects' rights with respect to their Personal Data under Data Protection Laws.

4.7. Provider will provide the Customer with the evidence about Provider's compliance with its obligations under this DPA and the applicable Data Protection Laws, such as summary reports related to SOC II Type 2 or ISO27001 security audits, or equivalent, upon Customer's request and no more than once per year unless the request is related to a Personal Data Breach or regulatory inquiry related to the Customer's use of the Services.

4.8. At the choice of Customer, Provider will, upon request, delete or return to Customer all Customer Personal Data within thirty (30) days after the end of the provision of the Services to Customer and delete existing copies unless applicable law requires retention of Personal Data.

4.9. Provider will notify Customer promptly if the Provider becomes actually aware of a Personal Data Breach, provided that the provision of such notice or any response by the Provider will not be construed as an acknowledgment of fault or liability with respect to any such Personal Data Breach.

4.10. Provider will use appropriate technical and organizational measures to protect Customer's Personal Data that will meet or exceed the requirements contained (a) under Data Protection Law, and (b) Schedule B to this DPA. Customer acknowledges that the security measures described in Schedule B are subject to technical progress

and development and that Provider may update or modify the security measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

5. EU Personal Data Processing Covenants

5.1. Without limitation to Section 4, in processing Personal Data relating to data subjects located in the European Economic Area ("**EU Personal Data**"), the following additional terms will apply:

a) Provider must, taking into account the nature of processing and the information available to the Provider, use commercially reasonable efforts to assist Customer, at Customer's expense, in ensuring compliance with Customer's obligations described in Articles 32 through 36 of the GDPR; and

b) Provider must make available upon Customer's reasonable request information reasonably necessary to demonstrate material compliance with the obligations in this DPA and allow for and contribute to audits (each, an "**Audit**"), at Customer's expense, including inspections of processing facilities under the Provider's control, conducted by Customer or another auditor chosen by Customer (an "**Auditor**"), during normal business hours and after reasonable prior notice, provided that no Auditor will be a competitor of the Provider, and provided further that in no event will Customer have access to the information of any other client of the Provider and the disclosures made pursuant to this Section 5.1(b) ("**Audit Information**") will be held in confidence as the Provider's confidential information and subject to any confidentiality obligations in the Agreement, and provided further that no Audit will be undertaken unless or until Customer has requested, and the Provider has provided, documentation pursuant to this Section and Customer reasonably determines that an Audit remains necessary to demonstrate material compliance with the obligations in this DPA. Without limiting the generality of any provision in the Agreement, Customer must employ the same degree of care to safeguard Audit Information that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer will be liable for any improper disclosure or use of Audit Information by Customer or its agents.

6. Subprocessors

6.1. Subprocessors assist the Provider in processing Personal Data as set out in this DPA. The Provider will enter into contractual arrangements with subprocessors requiring the same level of data protection compliance and information security as provided for in this DPA. By entering into the Agreement and this DPA, Customer consents to the processing of Personal Data by the disclosure and transfer of Personal Data to the subprocessors listed at https://legal.signnow.com/subprocessors ("**Subprocessor List**"). The Provider will inform the Customer about any intended changes to add or replace subprocessors in its Subprocessor List by posting an updated list of subprocessors at least ten (10) calendar days before the new subprocessor processes EU Personal Data.

6.2. Customer may object to such changes in writing within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection (an "**Objection**") by submitting SignNow Subprocessor Action Form. In the event of an Objection, the parties will discuss such concerns in good faith with the intention of achieving a resolution. If the parties are not able to achieve a resolution as described in the previous sentence, Customer, as its sole and exclusive remedy, may terminate the Agreement for convenience, on the condition that Customer provides written notice to the Provider within five (5) calendar days of being informed of the engagement of the subprocessor. Customer will not be entitled to any refund of fees paid prior to the date of any termination pursuant to this Section.

7. Data Transfers

7.1. Customer consents to the transfer to and the processing of EU Personal Data in the United States of America.

7.2. **Transfers from the EEA.** Where a Restricted Transfer is made from the EEA, the EU SCCs are incorporated into this DPA and apply to the transfer as follows:

a) With respect to Restricted Transfers from Customer to Provider, Module One applies where both Customer and Provider are Controllers, Module Two applies where Customer is a Controller and Provider is a Processor, and Module Three applies where both Customer and Provider are Processors.

b) In Clause 7, the optional docking clause does not apply;

c) In Clause 9 of Modules Two and Three, Option 2 applies, and the period for prior notice of subprocessor changes is specified in Section 6 of this DPA.

d) In Clause 11, the optional language does not apply

e) In Clause 17, Option 1 applies with the governing law that is designated in the Choice of Law; Venue section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland, or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of England and Wales.

f) In Clause 18(b), disputes will be resolved before the courts in the applicable venue of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the courts of England and Wales will have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

g) Annex I of the SCCs is completed with the information in Schedule A to this DPA; and

h) Annex II of the SCCs is completed with the information in Schedule B to this DPA, and Annex III of the SCCs is completed with the information in the Subprocessors List.

7.3. **Transfers from Switzerland.** In case of any transfers of Data from Switzerland, (a) general and specific references in the EU SCCs to GDPR or EU or Member State Law have the same meaning as the equivalent reference in the Swiss DPA, as applicable; and (b) any other obligation in the EU SCCs determined by the Member State in which the data exporter or Data Subject is established refer to an obligation under Swiss DPA, as applicable.

7.4. **Transfers from the UK.** Where a Restricted Transfer is made from the UK, the UK Transfer Addendum is incorporated into this DPA and applies to the transfer. The UK Transfer Addendum is completed with the information in Section 7.2, the Subprocessors List, and Schedules A and B to this DPA; and both "Importer" and "Exporter" are selected in Table 4.

7.5. If Provider adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to Data Protection Law) for the transfer of personal data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism will apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Law and extends to the territories to which Personal Data is transferred).

8. Miscellaneous

8.1. The terms of this DPA will control to the extent there is any conflict between the terms of this DPA and the terms of the Agreement. If there is any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail with respect to EU, Swiss, or UK Personal Data. Except as specifically amended and modified by this DPA, the terms and provisions of the Agreement remain unchanged and in full force and effect. Except as outlined in Section 3 of this DPA, the obligations contained in this DPA are (a) subject to any limitations of liability outlined in the Agreement, and (b) in addition to the other obligations contained in the Agreement. This DPA may be executed electronically, including using the Provider's electronic signature Services.

Schedule A: Processing Details

Parties

Data Importer: **airSlate, Inc.**
Address: 17 Station Street, Ste. 303
Brookline, MA 02445
Contact Name: N/A
Position: General Counsel
Contact: legal@airslate.com
Role: Processor/Controller

Data Exporter:
Address:
Contact Name:
Position:
Contact:
Role: Controller

Processing and Transfers

- **Categories of Data Subjects whose Personal Data is Transferred**

  Representatives of Customer; representatives of partners; Services users and visitors, including without limitation recipients of files uploaded into the Services; and individuals referenced in files uploaded into the Services.

- **Categories of Personal Data Transferred**

  EU Personal Data relating to the category of data subjects described above. The EU Personal Data depends on the particular Services but could include: Name, email address, demographic data, IP address, employer, address, geolocation, telephone number, occupation, and position, and any EU Personal Data provided by Customer and Services users and Services visitors (including without limitation recipients of files uploaded into the Services) in connection with the Services, including Customer Personal Data contained within files uploaded into the Services.

- **Sensitive Data Transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

  The contents of the Personal Data are varied and under the data exporter's control, but may, from time to time, depending on the particular Services, include sensitive data under the relevant Data Protection Laws.

- **Transfer Frequency**

  Transfers will be continuous for the duration necessary for the performance of the Services, any other purposes stipulated in the Agreement, and in compliance with applicable laws and regulations.

- **Nature of the Processing**

  The EU Personal Data will be subject to basic processing, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction for the purpose of providing Services by the Provider to Customer in accordance with the terms of the Agreement.

- **Transfer Purpose(s)**

  EU Personal Data will be subject to those Processing operations described in the Agreement.

- **Retention Period or Its Criteria**

  While providing such Services to Customer, Provider will Process EU Personal Data as instructed by Customer for the duration of the Agreement.

- **Transfers to Subprocessors**

  All authorized subprocessors are required to implement and maintain the same or substantially similar technical and organizational measures, responsibilities, and obligations as those required of Provider under this DPA.

- **Business Purpose(s) for Processing of California Consumers' Personal Information**
  For processing involving California consumers, only the following and checked business purpose(s) for processing personal data apply:

☒ Helping to ensure security and integrity to the extent that the use of the consumer's personal information is reasonably necessary and proportionate for these purposes

☒ Debugging to identify and repair errors that impair existing intended functionality.

☒ Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

☒ Undertaking internal research for technological development and demonstration.

☒ Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

☒ To retain and employ another service provider or contractor as a subcontractor where the subcontractor meets the requirements for a service provider or contractor under CCPA.

☒ To build or improve the quality of the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by CCPA, provided that the Service Provider does not use the Personal Data to perform services on behalf of another person.

☒ To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity, even if this Business Purpose is not specified in the written contract.

☐ Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

☐ Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

☐ Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor will not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

Competent Supervisory Authority

- Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 regarding the data transfer shall act as a competent supervisory authority.

- Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established will act as the competent supervisory authority.

- Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without, however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Data Protection Commission (DPC) – 21 Fitzwilliam Square, South Dublin 2, D02 RD28 Ireland will act as the competent supervisory authority.

- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office will act as the competent supervisory authority.

- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner will act as the competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

Schedule B: Security Measures

- **Program.** Provider will implement and maintain a written information security program ("**Information Security Program**"), which contains reasonably appropriate administrative, technical, and organizational safeguards that comply with this Schedule.

- **Access Controls.** Provider will implement measures to: (a) abide by the "principle of least privilege," pursuant to which access to Personal Data by Provider personnel will be limited on a need-to-know basis; and (b) promptly terminate its personnel's access to Personal Data when such access is no longer required for performance under the Agreement.

- **Account Management.** Provider will manage the creation, use, and deletion of all account credentials used to access the Provider's key infrastructure, including requiring multi-factor authentication in all critical systems.

- **Vulnerability Management.** Provider will (a) periodically use automated vulnerability scanning tools to scan the Provider's production system for vulnerabilities, including but not limited to penetration testing, and (b) implement patch management and software update tools as notified by the providers of those tools.

- **Security Segmentation.** Provider will monitor, detect, and restrict the flow of information on a multilayered basis using tools such as firewalls, proxies, and network-based intrusion detection systems.

- **Data Loss Prevention.** Provider will use loss prevention measures to identify, monitor, and protect Personal Data in use, in transit, and at rest. Such data loss prevention processes and tools will include: (a) automated tools designed to identify attempts of data exfiltration; and (b) the use of encryption certificate-based security.

- **Encryption.** Provider will encrypt, using industry-standard encryption tools, all Personal Data that Provider transmits across public networks.

- **Pseudonymization.** Provider will use industry-standard pseudonymization techniques to protect Personal Data where possible and consistent with the Services.

- **Physical Safeguards.** Provider will maintain physical access controls to secure the Provider-owned physical premises where the relevant Provider computing environment used to Process any Personal Data is located, including an access control system that enables Provider to control physical access to each Provider facility.

- **Administrative Safeguards.** Prior to providing access to Customer Personal Data to any of its personnel, Provider will use commercially reasonable measures: (a) verify the reliability of such personnel; and (b) provide appropriate security training to such personnel.